Can. J. Math., Vol. XXXVIII, No. 4, 1986, pp. 925-936.

THE SMALLEST PRIME VALUE OF $x^n + a$

KEVIN S. McCURLEY

1. Introduction. Let a and n be positive integers such that $f(x) = x^n + a$ is irreducible over the integers. A conjecture made by Bouniakowsky [**4**] in 1857 would imply that there exist infinitely many integers x such that $f(x)$ is prime. An even stronger conjecture of Bateman and Horn [**1**, **2**] would imply that

$$\pi(x; f) \sim \frac{C(f)}{n} \frac{x}{\log x} \quad \text{as } x \to \infty,$$

where $\pi(x; f)$ is the number of integers m with $0 \leqq m \leqq x$ for which $f(m)$ is prime, and

$$C(f) = \prod_p \frac{p - w(p)}{p - 1},$$

where $w(p)$ is the number of solutions of the congruence

$$x^n \equiv -a (\text{mod } p).$$

Except for the trivial case $n = 1$, neither of these conjectures has ever been resolved.

If Bouniakowsky's conjecture is true, then it seems natural to inquire about the size of the smallest nonnegative integer x for which $f(x)$ is prime. In this paper we prove that there exist irreducible polynomials of the form $x^n + a$ whose smallest prime value is large as a function of the parameters a and n. A result of this type was proved by the author in a previous paper [**8**]. For a statement of this result, we require the following definition.

Definition. Let

$$g(x) = \sum_{k=0}^{n} a_k x^k$$

be a polynomial with integral coefficients. The length of g, written $L(g)$, is defined as

Received December 13, 1984 and in revised form May 31, 1985.

$$L(g) = \sum_{k=0}^{n} ||a_k||,$$

where $||a_k||$ is the number of digits in the binary representation of a_k, with $||0|| = 1$.

Throughout this paper we use $C_1, C_2, \ldots$ to represent positive absolute constants, and $\log_k x$ to represent the k-fold iterated natural logarithm of x. The following result is due to the author [**8**].

THEOREM 1. *There exist infinitely many irreducible polynomials of the form $f(x) = x^n + a$ such that $f(x)$ is composite for all integers x with*

$$|x| < \exp\left(\exp\left(C_1 \frac{\log L(f)}{\log_2 L(f)}\right)\right).$$

This result has an interesting connection with an algorithm proposed by Brillhart [**5**] for proving that a polynomial is irreducible over the integers. Brillhart's algorithm involves locating a suitable prime value of the polynomial, and the polynomials of Theorem 1 provide examples where the simplest form of Brillhart's algorithm will not terminate in polynomial time. It should be noted that this observation is primarily of theoretical interest, and that variations of Brillhart's algorithm probably work well in practice. For a more thorough discussion of this, consult Brillhart's original paper or the author's paper [**8**] and the references listed there.

The proof of Theorem 1 uses a lemma due to A. Odlyzko stating that there exist infinitely many integers n having at least $\exp(C_2 \log n/\log_2 n)$ divisors of the form $p - 1$, where p is a prime. As a result, Theorem 1 applies only to a very restricted set of degrees n. In this paper we use different methods to prove two results that are valid for all n.

It is easy to prove that for any fixed n and u, there exists a positive integer a such that $x^n + a$ is irreducible over the integers and $x^n + a$ is composite for all integers x with $0 \leqq x \leqq u$. The following result gives an estimate for the least value of a for which this is true. In what follows, $d(n)$ is used to denote the number of positive integral divisors of n.

THEOREM 2. *There exists a positive absolute constant C_3 such that for every integer $n \geqq 2$, and $u \geqq 2$, there exists a positive integer a with*

$$0 < a < \exp[\exp(u^{1/d(n)} n^{C_3})]$$

such that $x^n + a$ is irreducible over the integers and $x^n + a$ is composite for all integers x with $0 \leqq x \leqq u$. If there do not exist any Siegel zeros (see Section 2) then there exists such an integer a with

https://doi.org/10.4153/CJM-1986-045-9 Published online by Cambridge University Press

$$0 < a < \exp[\exp(C_4 u^{1/d(n)} \log n)],$$

where once again C_4 is absolute.

The proof of Theorem 1 shows that $x^n + a$ may have no small prime value in the case where n has many divisors of the form $p - 1$, where p is a prime. It follows from Theorem 2 that the same is true if n merely has a large number of divisors. Suppose that n is a large integer with

$$d(n) > \exp(C_5 \log n/\log_2 n)$$

for some constant C_5, and that no Siegel zeros exist. By choosing $u = e^{d(n)}$ in Theorem 2, we find that there exists an irreducible polynomial $f(x) = x^n + a$ such that $f(x)$ is composite for all integers x with

$$0 \leqq x \leqq \exp[\exp(C_6 \log L(f)/\log_2 L(f))].$$

Except possibly for the size of the constant C_6, this would extend Theorem 1 to cover a larger class of degrees n.

Theorem 2 gives an estimate that is uniform in u and n. For fixed n and large values of u, the following result gives an improvement over Theorem 2.

THEOREM 3. *For every integer $n \geqq 1$, there exists a positive constant $C(n)$, and infinitely many integers a such that $x^n + a$ is irreducible over the integers, and $x^n + a$ is composite for all integers x with*

$$0 \leqq x \leqq C(n)\frac{\log a}{\log_3 a}\left(\frac{\log_2 a \log_4 a}{\log_3 a}\right)^{d(n)}.$$

Rankin [**10**] was the first to prove this result in the case $n = 1$, but the cases $n > 1$ appear to be new. In the case $n = 1$, Rankin's result shows that if p_k is the k^{th} prime and $\epsilon > 0$, then

$$(1) \quad p_{k+1} - p_k > (e^\gamma - \epsilon)\log k\frac{\log_2 k \log_4 k}{(\log_3 k)^2}$$

for infinitely many integers k. In passing we note that P. Erdös has offered ten thousand dollars for a proof of (1) with e^γ replaced by a function that tends to infinity with k.

The proof of Theorem 3 is a generalization of the method of Rankin, and gives

$$C(1) = e^\gamma - \epsilon \quad \text{and} \quad C(2) = (2e^{2\gamma}/\pi^2) - \epsilon,$$

for any $\epsilon > 0$, provided a is sufficiently large. If $n \geqq 3$ then $C(n)$ does not have such a simple form, and the problem of estimating $C(n)$ as a function of n is essentially equivalent to the estimation of a in Theorem 2.

It is probably a very difficult question to determine how close these results are to best possible. In Section 5 we present some numerical

examples, with the hope that they may prove illustrative in future investigations.

2. Preliminary lemmas. In what follows, p always represents a prime, and (x, y) represents the greatest common divisor of x and y.

LEMMA 1. *There exists a positive constant C_7 such that*

$$\sum_{p \leqq y} \frac{1}{p} = \log_2 y + C_7 + O\left(\frac{1}{\log y}\right)$$

provided $y \geqq 2$.

Proof. See [7], p. 151.

LEMMA 2. *Let $\psi(x, y)$ be the number of integers m with $1 \leqq m \leqq x$ having no prime factor exceeding y, and fix $\epsilon > 0$. Then*

$$\psi(x, y) < x \exp(-(1 - \epsilon)t \log t),$$

where $t = \log x/\log y$, provided $t \leqq (\log x)^{1/3}$ and x is sufficiently large.

Proof. See [6].

Let $(k, l) = 1$, and define

$$\theta(x; k, l) = \sum_{\substack{p \leqq y \\ p \equiv l (\mathrm{mod} k)}} \log p.$$

The proofs of Theorems 2 and 3 use estimates for $\theta(x; k, l)$ that depend upon information concerning the location of zeros of Dirichlet L-functions. If χ is a character modulo k and $L(s, \chi)$ is the associated Dirichlet L-function, then it is well known (see for example [3], p. 39) that

$$L(\sigma + it, \chi) \neq 0 \quad \text{for } \sigma > 1 - C_8/\log[k(2 + |t|)],$$

except possibly when χ is real-valued, when there may be a single real zero. Such zeros have come to be known as Siegel zeros or exceptional zeros, but it is widely believed that none exist. The following result gives a useful estimate for $\theta(x; k, l)$ in the case that Siegel zeros do not exist.

LEMMA 3. *Let k be a modulus for which there do not exist any Siegel zeros, and let $(k, l) = 1$. Then there exist constants C_9, C_{10}, and $D = D(C_8)$ such that*

$$\theta(x; k, l) = \frac{x}{\varphi(k)} + O\left(\frac{x}{\varphi(k)} \exp(-C_9\sqrt{\log x})\right) + O\left(\frac{x^{1 - C_{10}/\log k}}{\varphi(k)}\right),$$

provided $x \geqq k^D$.

https://doi.org/10.4153/CJM-1986-045-9 Published online by Cambridge University Press

Proof. This follows from an argument of Bombieri [**3**, p. 54-55], with the choice

$$T = k \exp((\log x)^{1/2}).$$

LEMMA 4. *Let $y \geqq 2$, $(k, l) = 1$, and let $p_1(k, l)$ be the least prime congruent to l modulo k. Then*

$$\sum_{\substack{p \leqq y \\ p \equiv l (\mathrm{mod} k)}} \frac{1}{p} = \frac{\log_2 y}{\varphi(k)} + \frac{1}{p_1(k, l)} + O\left(\frac{\log k}{\varphi(k)}\right) \tag{2}$$

where the implied O-constant is absolute. If in addition there are no Siegel zeros for the modulus k, then there exists an absolute constant C_{11} such that

$$\sum_{\substack{p \leqq y \\ p \equiv l (\mathrm{mod} k)}} \frac{1}{p} \geqq \frac{\log_2 y}{\varphi(k)} - \frac{\log_2 k}{\varphi(k)} - \frac{C_{11}}{\varphi(k)}. \tag{3}$$

Proof. The first statement is due to K. K. Norton [**9**]. It is interesting to note that by using the Siegel-Walfisz Theorem in Norton's proof, one can replace the log k term by $\epsilon \log k$, provided k exceeds some (ineffective) bound depending on ϵ. In addition to (2), Norton proved that if there are no Siegel zeros, then log k can be replaced by $\log_2 k$.

We now prove (3). Note that from Lemma 3 it follows that if $x \geqq k^D$, then

$$\theta(x; k, l) = \frac{x}{\varphi(k)} + O\left(\frac{x}{\varphi(k) \log x}\right) + O\left(\frac{x^{1 - C_{10}/\log k}}{\varphi(k)}\right). \tag{4}$$

If $y < k^D$, then (3) is trivial, provided that $C_{11} > \log D$. If $y \geqq k^D$, then from (4) we obtain

$$\begin{aligned}
\sum_{\substack{p \leqq y \\ p \equiv l (\mathrm{mod} k)}} \frac{1}{p} &= \int_{1-}^{y} \frac{d\theta(t; k, l)}{t \log t} \\
&= \frac{\theta(y; k, l)}{y \log y} + \int_1^y \frac{\theta(t; k, l)(1 + \log t)dt}{t^2 \log^2 t} \\
&\geqq \int_{k^D}^{y} \frac{\theta(t; k, l)}{t^2 \log t} dt \\
&\geqq \frac{\log_2 y - \log_2(k^D)}{\varphi(k)} \\
&\quad - \frac{C_{12}}{\varphi(k)} \int_{k^D}^{y} \left(\frac{1}{t \log^2 t} + \frac{t^{-C_{10}/\log k}}{t \log t}\right) dt.
\end{aligned}$$

https://doi.org/10.4153/CJM-1986-045-9 Published online by Cambridge University Press

The last integral satisfies

$$\int_{k^D}^{y} \frac{t^{-C_{10}/\log k}}{t \log t} dt < \frac{1}{D \log k} \int_{k^D}^{y} t^{-1-C_{10}/\log k} dt = O(1),$$

which proves the lemma if C_{11} is sufficiently large.

LEMMA 5. *There exists a positive constant C_{13} such that*

$$(5) \quad \prod_{p \leqq y} \frac{p-1}{p-1+(p-1,n)} < \exp(C_{13} d(n) \log n - d(n) \log_2 y),$$

provided $y \geqq 2$. If there do not exist any Siegel zeros for moduli d that are divisors of n, then there exists a constant C_{14} such that

$$(6) \quad \prod_{p \leqq y} \frac{p-1}{p-1+(p-1,n)} < \exp(d(n) \log_2 n + C_{14} d(n) - d(n) \log_2 y).$$

Proof. From the inequality $\log(1+x) > x - x^2/2$ it follows that

$$(7) \quad \log\left(\frac{p-1}{p-1+(p-1,n)}\right) < \log\left(\frac{p}{p+(p-1,n)}\right) < \frac{-(p-1,n)}{p} + \frac{(p-1,n)^2}{2p^2}.$$

We now observe that

$$(8) \quad \sum_{p \leqq y} \frac{(p-1,n)^2}{p^2} = \sum_{d \mid n} d^2 \sum_{\substack{p \leqq y \\ (p-1,n)=d}} \frac{1}{p^2} < \sum_{d \mid n} d^2 \sum_{k=1}^{\infty} \frac{1}{(kd)^2} < 2d(n).$$

From Lemma 4 we obtain

$$\sum_{p \leqq y} \frac{(p-1,n)}{p} = \sum_{p \leqq y} \frac{1}{p} \sum_{d \mid (p-1,n)} \varphi(d) = \sum_{d \mid n} \varphi(d) \sum_{\substack{p \leqq y \\ p \equiv 1 \pmod d}} \frac{1}{p} \geqq \sum_{d \mid n} \varphi(d) \left(\frac{\log_2 y}{\varphi(d)} - \frac{C_{15} \log d}{\varphi(d)}\right) \geqq d(n) \log_2 y - C_{15} d(n) \log n.$$

https://doi.org/10.4153/CJM-1986-045-9 Published online by Cambridge University Press

Furthermore, if there are no Siegel zeros for moduli that are divisors of n, then from Lemma 4 we obtain

$$\sum_{p \leqq y} \frac{(p-1, n)}{p} \geqq d(n) \log_2 y - d(n) \log_2 n - C_{11} d(n).$$

Combining these estimates with (7) and (8) proves the lemma.

Note that for fixed n, and for y tending to infinity, the inequalities (5) and (6) can be replaced by an asymptotic result with an appropriate constant. If $n = 1$, then (5) can be replaced by a result of Merten's (see [7]) that

$$\prod_{p \leqq y} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log y}.$$

Furthermore, if $n = 2$, then (5) becomes

$$(9) \quad \frac{3}{2} \prod_{p \leqq y} \frac{p-1}{p+1} \sim \frac{3}{2} \prod_{p} (1 - p^{-2})^{-1} \prod_{p \leqq y} (1 - p^{-1})^2 \sim \frac{\pi^2}{4e^{2\gamma} \log^2 y}.$$

3. Proof of theorem 2. Let

$$w = \exp\{(1+u)^{1/d(n)} n^{C_{16}}\},$$

let q be the least prime exceeding w, and let $p_1, p_2, \ldots, p_t$ be the primes less than w. Our goal is to choose $a > w$ in such a way that $x^n + a$ is irreducible in $\mathbf{Z}[x]$, and such that if $0 \leqq x \leqq u$, then $x^n + a$ is divisible by a prime less than w, hence composite. We do this by choosing a as a solution to a congruence modulo $Q = q^2 \prod p_i$, with $Q < a < 2Q$. We begin by choosing $a \equiv q (\mathrm{mod}\ q^2)$, so that $x^n + a$ is irreducible by Eisenstein's criterion.

Beginning with p_1, and proceeding through the primes in increasing order, we choose a modulo p_k in such a way that $m^n \equiv -a (\mathrm{mod}\ p_k)$ has a maximal number of solutions m among those m's that do not satisfy a congruence

$$m^n \equiv -a (\mathrm{mod}\ p_i), \quad i < k.$$

Let $N_0 = 1 + [u]$, and let N_k be the number of m's with $0 \leqq m \leqq u$ such that $m^n + a$ is not divisible by a prime $p \leqq p_k$. Since the function $h(x) = x^n$ takes on only $1 + (p_k - 1)/(p_k - 1, n)$ values modulo p_k, (see [7], p. 90-91) we have

$$m^n + a \equiv 0 (\mathrm{mod}\ p_k)$$

https://doi.org/10.4153/CJM-1986-045-9 Published online by Cambridge University Press

for at least $N_{k-1}/\{1 + (p_k - 1)/(p_k - 1, n)\}$ of the numbers counted in N_{k-1}. Hence

$$N_k < N_{k-1}\left(\frac{p_k - 1}{p_k - 1 + (p_k - 1, n)}\right)$$
$$< N_0 \prod_{p \leqq p_k} \left(\frac{p - 1}{p - 1 + (p - 1, n)}\right).$$

It now follows from Lemma 5 that

$$N_t < (1 + u)\exp(C_{13}d(n) \log n - d(n) \log_2 w) < 1,$$

if C_{16} is large. Since N_t is an integer, it follows that $N_t = 0$, and $x^n + a$ is composite for $0 \leqq x \leqq u$. Note that

$$a < 2Q = 2q^2 \prod_{p<w} p$$
$$< \exp(2w),$$

if w is sufficiently large (which can be accomplished by taking C_{16} large). It then follows that

$$a < \exp(\exp(u^{1/d(n)}n^{C_3})),$$

provided C_3 is sufficiently large.

Let us now assume that there are no Siegel zeros. In this case we take

$$w = \exp(C_{17}(1 + u)^{1/d(n)}\log n).$$

We then get

$$N_t < (1 + u)\exp(d(n) \log_2 n + C_{14}d(n) - d(n) \log_2 w) < 1,$$

if C_{17} is sufficiently large. It remains only to observe that $a < \exp(2w)$ for w sufficiently large, so that

$$a < \exp(\exp(C_3u^{1/d(n)} \log n))$$

for C_3 sufficiently large.

4. Proof of theorem 3. Let n be fixed, $\epsilon > 0$ be small, and let w be large. Let q be the least prime exceeding w, and let

$$u = \alpha\frac{w}{\log_2 w}\left(\frac{\log w \log_3 w}{\log_2 w}\right)^{d(n)},$$

where α is a constant to be chosen later. As in the proof of Theorem 2, we choose a modulo $Q = q^2 \prod p_i$, where p_i runs over all primes less than w. We also take $Q \leqq a < 2Q$ and $a \equiv q \pmod{q^2}$, so that $x^n + a$ is irreducible. Note that it follows from the Prime Number Theorem that $\log a \sim w$ as $w \to \infty$.

https://doi.org/10.4153/CJM-1986-045-9 Published online by Cambridge University Press

Define

$$y = \exp\left((1 - 2\epsilon)\frac{\log w \log_3 w}{\log_2 w}\right),$$

$$z = \frac{w}{\log_2 w}.$$

If $y < p \leqq z$, then we choose $a \equiv 0 (\mathrm{mod}\ p)$. Consider now the set of integers m with $0 \leqq m \leqq u$ for which $m^n + a$ is not divisible by a prime between y and z. These m's are of two types:

i) m is only divisible by primes not exceeding y

ii) m is divisible by at least one prime exceeding z.

Let S_1 and S_2 be the number of m's of types i) and ii), respectively. From Lemma 1 we obtain

$$\begin{aligned} S_2 &\leqq \sum_{z<p\leqq u} \left[\frac{u}{p}\right] \leqq u \sum_{z<p\leqq u} \frac{1}{p} \\ &< u\left(\log_2 u - \log_2 z + O\left(\frac{1}{\log z}\right)\right) \\ &< (1 + \epsilon)d(n)u\frac{\log_2 w}{\log w}, \end{aligned}$$

for w sufficiently large. Furthermore since $S_1 = \psi(u, y)$, Lemma 2 yields

$$\begin{aligned} S_1 &< u \exp\left[-(1 - \epsilon)\frac{\log u}{\log y}\log\left(\frac{\log u}{\log y}\right)\right] \\ &< \frac{u}{\log w}, \end{aligned}$$

for w sufficiently large. It follows that

$$S_1 + S_2 < (1 + 2\epsilon)d(n)u\frac{\log_2 w}{\log w}.$$

We now choose a modulo p for all $p \leqq y$, using the same strategy as in the proof of Theorem 2. After doing so, the number of m's with $0 \leqq m \leqq u$ such that $m^n + a$ is not divisible by a prime less than z is at most

$$(S_1 + S_2)\prod_{p\leqq y}\frac{p - 1}{p - 1 + (p - 1, n)}.$$

Using Lemma 5, this quantity is bounded above by $C_{18}\alpha w/\log w$, where C_{18} is a constant depending on n and ϵ. With an appropriate choice of α, the number of surviving m's is less than

$$(1 - \epsilon)w/\log w.$$

https://doi.org/10.4153/CJM-1986-045-9 Published online by Cambridge University Press

If w is sufficiently large, then the number of primes between z and w exceeds the number of surviving m's, and for these primes p we can choose a modulo p in such a way as to remove at least one m with each prime. The result is that every m with $0 \leqq m \leqq u$ satisfies at least one congruence

$$m^n + a \equiv 0 (\text{mod } p) \quad \text{with } p < w,$$

and this completes the proof of Theorem 3.

For $n = 1$, this is exactly the proof outlined by Rankin, and leads to

$$C(1) = e^{\gamma} - \epsilon \quad \text{for } a \geqq a_0(\epsilon).$$

Similarly if $n = 2$, we obtain from (9) that

$$C_{18} = \frac{(1 + 2\epsilon)\pi^2}{2(1 - 2\epsilon)^2 e^{2\gamma}} + \epsilon,$$

if w is sufficiently large. An appropriate choice of α then leads to

$$C(2) = (2e^{2\gamma}/\pi^2) - \epsilon \quad \text{if } a \geqq a_0(\epsilon).$$

5. Some numerical examples. It is widely believed that Theorem 3 can be substantially improved if $n = 1$, and there seems to be little reason to doubt that this is also the case for $n \geqq 2$. In this section we discuss some numerical examples of irreducible polynomials of the form $x^n + a$ that have no small primes values, with the hope that they may give some insight into the type of improvement that might be obtained for Theorem 3.

If $n \geqq 1$ and $a > 0$ are such that $x^n + a$ is irreducible, we define $R_n(a)$ to be the least nonnegative integer x such that $x^n + a$ is prime (such an x exists if Bouniakowski's conjecture is true). For fixed n we also define a sequence $a_0, a_1, \ldots$, where $a_0 = 7$ and a_k is the least positive integer such that $x^n + a_k$ is irreducible and $R_n(a_k) > R_n(a_{k-1})$. The numbers a_k are the places where $R_n(a)$ assumes a new maximum value. In Table 1-4 below we give all a_k less than a specified limit, along with $R_n(a_k)$, for $n = 2, 3, 4, 5$.

TABLE 1 ($n = 2$, all $a_k \leqq 10^6$)

a_k	$R_2(a_k)$	a_k	$R_2(a_k)$
7	0	749	60
8	3	3485	66
21	4	3561	70
24	7	6041	114
117	8	17531	150
119	12	43181	210
185	18	52454	225
341	36	159731	294
489	38	218084	357
545	42	576239	402

https://doi.org/10.4153/CJM-1986-045-9 Published online by Cambridge University Press

TABLE 2 ($n = 3$, all $a_k \leqq 10^6$)

a_k	$R_3(a_k)$	a_k	$R_3(a_k)$
7	0	1464	67
9	2	1490	69
14	3	2918	87
24	5	4031	122
50	11	35036	123
84	13	38583	136
111	20	56510	147
176	21	69152	153
246	23	88152	169
405	26	114360	179
685	28	291068	189
895	48	382108	297
1044	53		

TABLE 3 ($n = 4$, all $a_k \leqq 150000$)

a_k	$R_4(a_k)$	a_k	$R_4(a_k)$
7	0	959	540
8	3	2204	735
9	10	2369	840
14	165	9224	1275
74	255	12869	1380
189	290	18854	1755
524	315	72254	2505
584	435		

TABLE 4 ($n = 5$, all $a_k \leqq 10^5$)

a_k	$R_5(a_k)$	a_k	$R_5(a_k)$
7	0	736	175
8	3	5114	195
24	7	11142	209
33	8	13738	255
48	13	36213	268
54	17	46353	286
80	63	58752	295
122	75	60435	322
309	82	89750	339
318	83		

It is interesting to observe the wide variation in the rates of growth of $R_n(a)$ for different values of n. Roughly speaking, we might expect that $R_n(a)$ grows more rapidly the bigger n is, for the simple reason that the values of $x^n + a$ are larger and therefore less likely to be prime. On the other hand, it definitely appears from the data that $R_4(a)$ grows more

rapidly that $R_5(a)$, which suggests that the rate of growth may depend on some arithmetic property of n such as the size of $d(n)$. This may also explain why in Theorem 3 we are able to prove a stronger result for $n = 4$ than we are for $n = 5$.

The growth of $R_6(a)$ is even more startling, although the data is somewhat sketchy because of the large numbers involved. The following examples were discovered in a computer search conducted by the author.

$$\begin{aligned}
&x^6 + 2 && \text{composite for } |x| < 39,\\
&x^6 + 11, && \text{composite for } |x| < 54,\\
&x^6 + 20, && \text{composite for } |x| < 399,\\
&x^6 + 41, && \text{composite for } |x| < 546,\\
&x^6 + 272, && \text{composite for } |x| < 2163,\\
&x^6 + 5186, && \text{composite for } |x| < 3759,\\
&x^6 + 8546, && \text{composite for } |x| < 5859.
\end{aligned}$$

Here there is no claim made that the polynomials actually have a prime value at the endpoint of the interval, but only that the value N of the polynomial satisfies the congruence $2^N \equiv 2 (\text{mod } N)$, so that N is very likely to be prime.

References

1. P. Bateman and R. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. *16* (1962), 363-367.
2. ——— *Primes represented by polynomials in one variable*, Proc. Symp. Pure Math. *8* (1965), 119-135.
3. E. Bombieri, *Le grand crible dans la théorie analytique des nombres. Avec une sommaire en anglais*, Asterisque *18* (Société Mathématiques de France, Paris, 1974).
4. V. Bouniakowsky, *Sur les diviseurs numeriques invariables des fonctions rationelles entieres*, Mem. Acad. Sci. St. Petersburg *6* (1857), 305-329.
5. J. Brillhart, *Note on irreducibility testing*, Math. Comp. *35* (1980), 1379-1381.
6. N. G. de Bruijn, *On the number of positive integers* $\leqq x$ *and free of prime factors* $> y$, Nederl. Akad. Wetensch. Proc. Ser. A *54* (1951), 50-60.
7. W. J. LeVeque, *Fundamentals of number theory* (Addison-Wesley, Reading, MA, 1977).
8. K. S. McCurley, *Prime values of polynomials and irreducibility testing*, Bull. Amer. Math. Soc. (N.S.) *11* (1984), 155-158.
9. K. K. Norton, *On the number of restricted prime factors of an integer I*, Illinois J. Math. *20* (1976), 681-705.
10. R. A. Rankin, *The difference between consecutive prime numbers V*, Proc. Edinburgh Math. Soc. (2) *13* (1962/63), 331-332.

Michigan State University,
East Lansing, Michigan;
University of Southern California,
Los Angeles, California